Image Privacy Protection Using Visual Cryptographic Schemes

Report submitted for the fulfillment of the requirements for the degree of Bachelor of Technology in

Information Technology

Submitted by

KritiChatterjee
(11700214041)

Arghya Kamal Mitra
(11700214017)

Aishwarya Mukherjee
(11700214007)

Under the Guidance of …

Dr.Indrajit Pan
Assistant Professor, Department of Information Technology
RCC Institute of Information Technology, Kolkata

RCC Institute of Information Technology
Canal South Road, Beliaghata, Kolkata – 700 015
[Affiliated to West Bengal University of Technology]

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to **Dr. Indrajit Pan**
of the department of Information Technology, whose role as project guide was invaluable for the project. We are extremely thankful for the keen interest he took in advising us, for the books and reference materials provided for the moral support extended to us.

Last but not the least we convey our gratitude to all the teachers for providing us the technical skill that will always remain as our asset and to all non-teaching staff for the gracious hospitality they offered us.

Place: RCCIIT, Kolkata

Date: .....

.....

.....

.....

Department of Information Technology

RCCIIT, Beliaghata,

Kolkata – 700 015,

West Bengal, India

Approval

This is to certify that the project report entitled "Image Privacy Protection using Visual Cryptographic Schemes" prepared under my supervision by **KritiChatterjee**(11700214041)
Arghya Kamal Mitra(11700214017)**Aishwarya Mukherjee**(11700214007)
be accepted in partial fulfillment for the degree of Bachelor of Technology in Information Technology.

It is to be understood that by this approval, the undersigned does not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn thereof, but approves the report only for the purpose for which it has been submitted.

…….. … ……
Name & Designation of the HOD Name & Designation of Internal Guide

INDEX

PICTURE INDEX

ABSTRACT

Here we deal with **Visual cryptography** which is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

One of the best-known techniques has been credited to MoniNaor and Adi Shamir, who developed it in 1994.[1] They demonstrated a visual secret sharing scheme, where an image was broken up into *n* shares so that only someone with all *n* shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares.

1. INTRODUCTION

Visual cryptography is a technique in which a image is decomposed into shares and to recover the original image the shares are stacked without any need of complex computation. Privacy of images is a matter of prime concern now days. There are various methods for maintaining privacy of an image and visual cryptography is one such method. In this method shares of an image are created and securely stored in various databases in the form of QR code. This reduces the chance of eavesdropping during the transmission phase.

With the world being connected by computers , the companies are afraid of storing any sort of confidential data in the computers as there are chances that these data may get exposed. However the solution to this problem is to distribute the data at several places and destroy the original one. Whenever there is need for the actual data it could be reconstructed from distributed shares. Hence Secret Sharing provides confidentiality to a database. It aims to attain two goals:

- **Data Secrecy.**
- **Data Availability.**

Data Availability is a process of ensuring that data is available to the end users of the system. If availability was the only goal then simply duplicating the full data in n places would avoid the loss data up to n-1 places from removing the secret. However this would increase the threats also, capturing any one of the places can disclose the secret.

Data Secrecy is a process of restricting data. If secrecy was the only goal then the solution could be divided into n parts and stored in n places. This would give rise to the need of making all the n places accessible to retrieve the secret. If there would be any alteration or destruction of any one part the distributed information would be lost.

Secret Sharing hence provides secrecy in the face of the enemies and thus achieves data integrity and availability with the assistance off its shareholders. The general concept of secret sharing is that, it doesn't want information to be centralized at one point.

Visual Cryptography has become a much needed application for the following reasons:

- Perfect Secrecy: The underlying principle of encrypting the original image into shares is similar to one time pad. Visual Cryptography provides perfect privacy in a similar way as one time pad.
- Secure Decryption: As the computers of present time are insecure decrypting the shares may result in the leaking of the plain text and the purpose of a perfectly secure shame is defeated. The decryption is done by laws of physics and by human visual system i.e. eyes and brain, using properties of contrast. Contrast is an important parameter in determining the human visual scheme can differentiate grey levels.

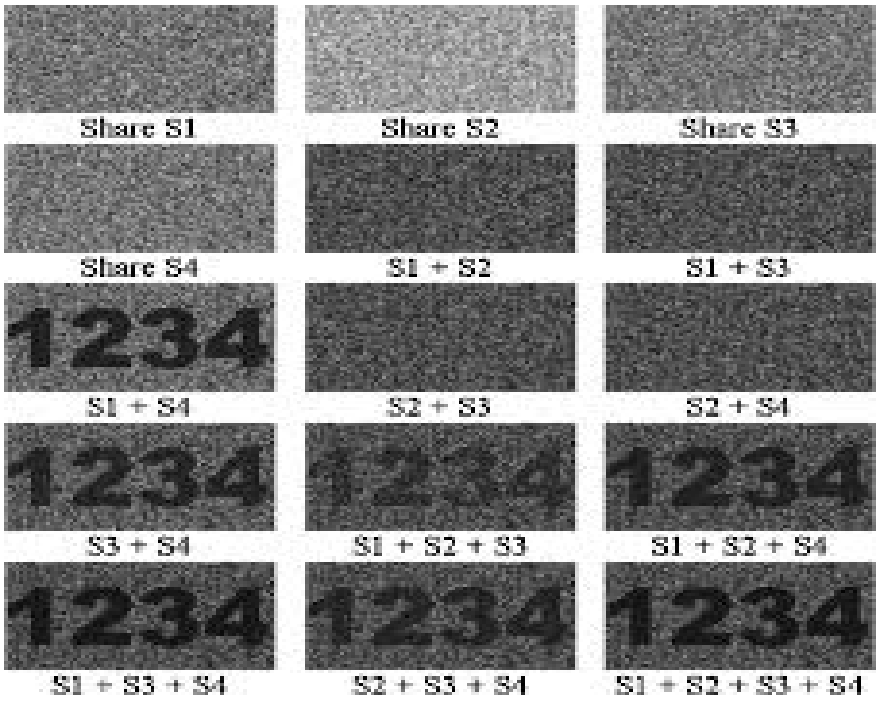

Fig1: An imageof share generation and stacked one upon the other to give rise to original image.

2. PROPOSED METHOD

There are different visual cryptographic schemes.

2.1IMPLEMENTATION OF VISUAL CRYPTOGRAPHY TO HIDE INFORMATION CONTAINED WITHIN AN IMAGE IN ANOTHER IMAGE

In this method of visual cryptography the following algorithm has been adopted

1. Check dimensions of both base and original image. If they are not equal then resize them.
2. Divide both base image and the cover image into 4x4 matrixes.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Fig2: Original Image(4x4)

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Fig3: Base Image(4x4)

3. Interchange the even cells of the base image with the even cells of the cover image.

1	B	3	D
5	F	7	H
9	J	11	L
13	N	15	P

Fig4: Interchanged even cells of base image with cover image

4. Slice and then interchange with reference to diagonal on both images.

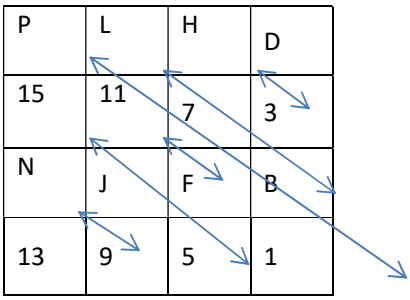

Fig5: Interchanged along the diagonal of the image

2.2 IMPLEMENTATION OF VISUAL CRYPTOGRAPHY BY SHARE GENERATION METHOD

One of the best-known techniques has been credited to MoniNaor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n -1 share revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out- of-n visual cryptography. Using a similar idea, transparencies can be used to implement a onetime pad encryption, where one transparency is a shared random pad, another transparency acts as the cipher text.

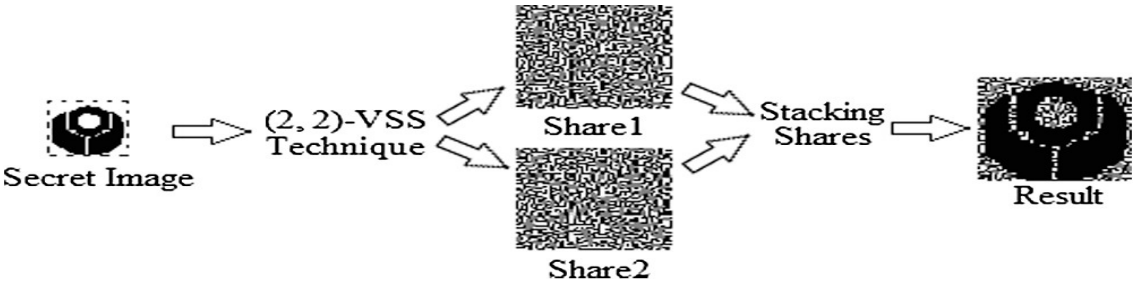

Fig6: Image depiction MoniNaor and Adi Shamir technique of visual cryptography.

3. EXPERIMENTAL RESULTS

3.1 VISUAL CRYPTOGRAPHY USING 2 IMAGES.

As described above, the visual scheme was implemented and gave the following results.

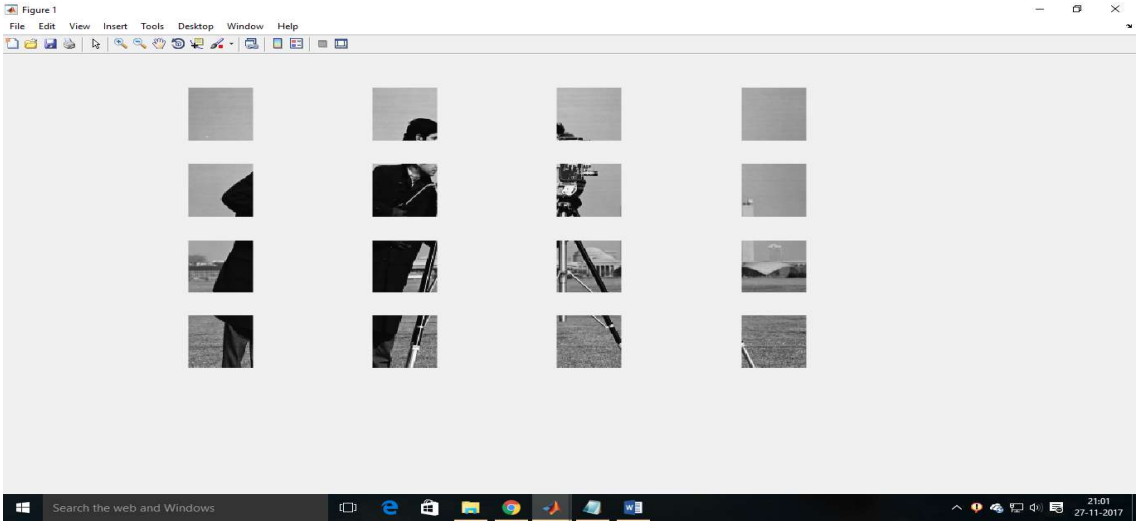

Fig7: The (4x4) matrix image of base image

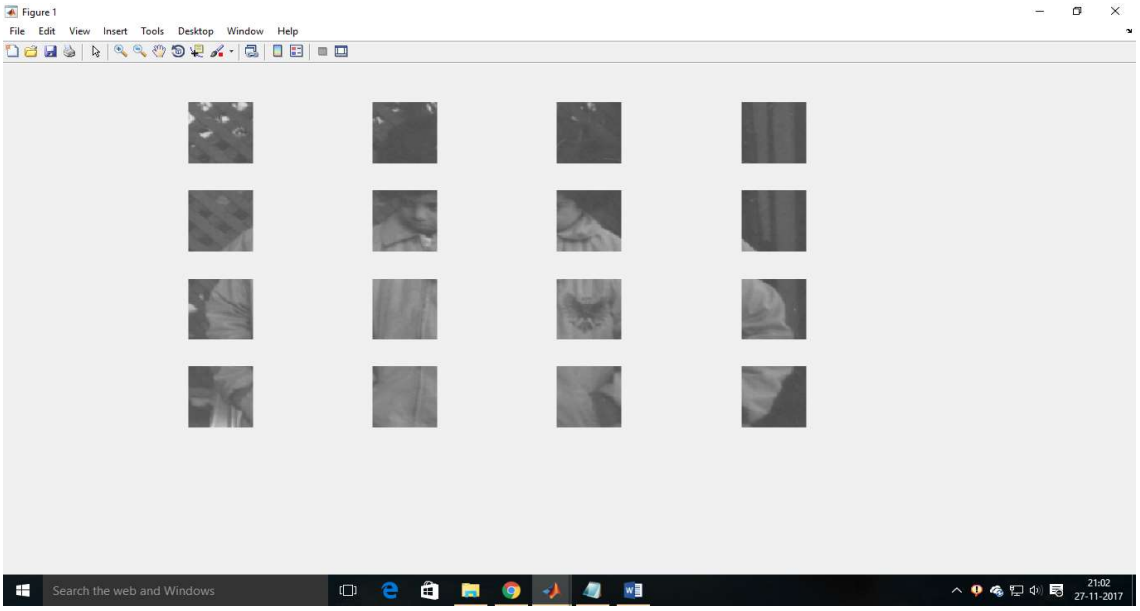

Fig8: The (4x4) matrix image of original image

The above method did not give desired results. Hence the following method of visual scheme was adopted.

3.2 VISUAL CRYPTOGRAPHY USING ADI SHAMIR AND MONI NAOR METHOD.

The above scheme is also called the share generation method because the procedure involves generation of shares by enlarging the pixels of an image and dividing each pixel into sub pixels and randomly dividing them into 2 shares.

Fig9: Original Image

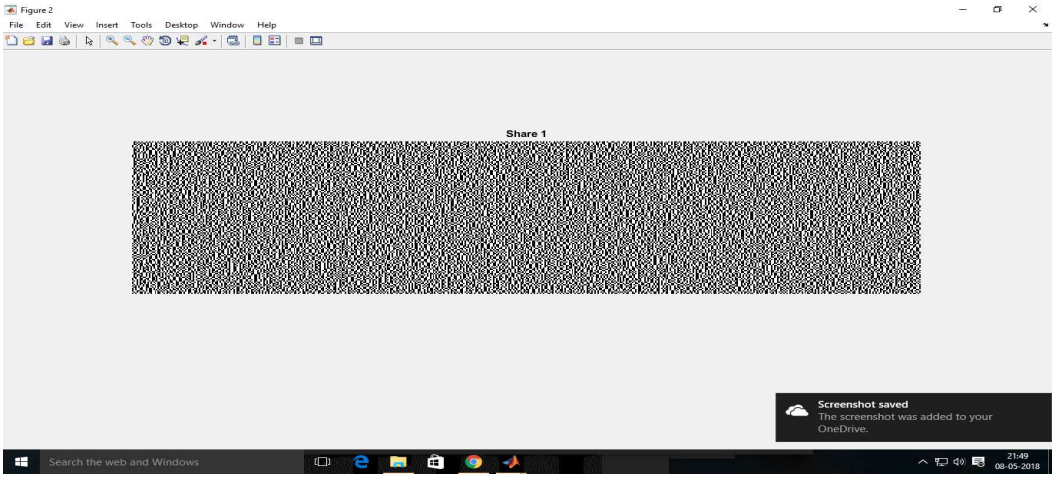

fig 10: share 1 generated from original image

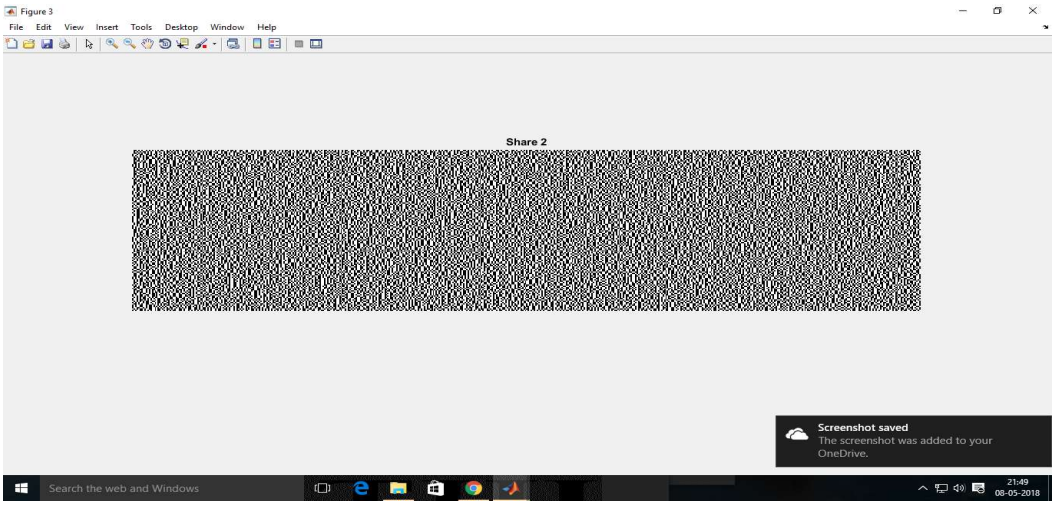

Fig 11:share 2 generated from original image

Fig12: The final image on overlapping of both shares

Fig13: Retrieval of original image.

4 CONCLUSIONS

Since its inception, cryptography has received considerable attention from researchers worldwide. Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Hence the information is secured, protected, confidential, authenticated and non-repudiated. Modern cryptography is based on computer science, mathematics and engineering. Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption is performed by the receiver while reading. Visual cryptography utilises the concept of concealing a secret data on the images with the help of noisy or random pixels. This technique makes it almost impossible to retrieve the hidden data from the image shared.

The advantage of visual cryptography scheme is that it eliminates computational problems or complex algorithms during the decryption process. The data hidden is decoded by stacking the shared images. The decryption is based on OR operation. Also, decryption is performed by human eye. Hence no expensive machineries is used or required. In current work, with the well-known n-k secret sharing visual cryptography scheme an enveloping technique is proposed where the secret shares are enveloped within apparently innocent covers of digital pictures using LSB replacement digital watermarking. This adds security to visual cryptography technique from illicit attack as it befools the hacker's eye.

The division of an image into n number of shares is done by using random number generator, which is a new technique not available till date. This technique needs very little mathematical calculations as opposed to those required in the present situation.

With the progress of science and technology, as more and more data is digitized, the hour is in need of more data security than it has ever been. Many applications of visual cryptography have been developed. Many authors have combined the use of both visual cryptography and steganography for copyright protection. The importance of using biometrics to establish personal authenticities ant to detect imposters is growing concern in the present scenario globally. The visual cryptographic can be used to detract hackers or third person entities that are ready to haunch upon the secret messages. Secure tongue biometric authentication system using visual cryptography is also an application of visual cryptography. Visual cryptography is also a powerful way of introducing a large audience to

the basic ideas of encryption and secure sharing in an unconditional secure and safe way. Also while an institution shares its visual shares of the password of a vault to a number of people, the visual cryptography technique can be used with some flexibility. In electronic voting schemes is also this method is used.

5 REFERENCES

1. Visual Cryptography for Image Privacy protection using Diverse Image media

JyotiRao and VikramPatil Research scholar of JJTU, Rajasthan, India

2. Hare Ram Sah Research Scholar, Faculty of Computer Science and Engineering, Sathyabama University, Chennai, India Dr. G.Gunasekaran Professor, Department of Computer Science and Engineering, Meenakshi College of Engineering,

3. MoniNaor and Adi Shamir, Department of Applied Math and Computer Science, Weizmann Institute, Rehovat-76100 on “Visual Cryptography”.

4.Paolo D’Arco and Roberto De Prisco, Department of Informatica, University of Salerno via Giovanni Paolo.Italyon”Visual Cryptography- Models,Issues,Applications and new directions”.

5. Monish Kumar Dutta and AshokeNath, Department of Computer Science, Kolkata, India on “scopes and challenges on visual cryptography” in IJIRAE